PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2000-338869
(43)Date of publication of application : 08.12.2000

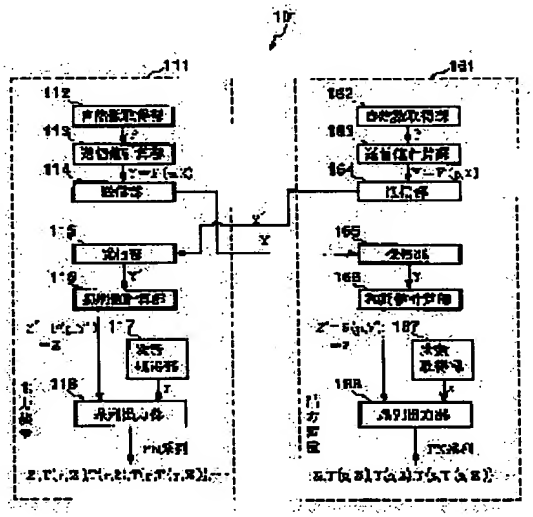
(51)Int.CI. G09C 1/00
H04J 13/00

(21)Application number : 11-152063
(22)Date of filing : 31.05.1999

(71)Applicant : COMMUNICATION RESEARCH LABORATORY MPT
UMENO TAKESHI
(72)Inventor : UMENO TAKESHI

(54) SYSTEM, DEVICES, AND METHOD FOR OUTPUTTING A PSEUDO NOISE SERIES, AND INFORMATION RECORDING MEDIUM

(57)Abstract:
PROBLEM TO BE SOLVED: To provide an output system for outputting a pseudo noise(PN) series by providing plural output devices based on a preset elliptic function, real number, a specific rational mapping, and a specific Chebyshev's mapping.
SOLUTION: PN series output devices 111, 116 are constituted based on a Chebyshev's mapping T (., .) defined by a preset elliptic function s (.), a real number X (however, $-1<X<1$), a rational mapping F (., .) defined by $F(n, s(x))=s(nx)$ ((n) is ≥2 of natural number), and $T(n, \cos x)=\cos(x)$. A transmission value calculating part 113 of the output device 111 and a transmission value calculation part 163 of the output device 161 calculate a value $Y=F(p, X)$ and a value $Y'=F(q, X)$ from a natural number (p) obtained by a natural number obtaining part 112 and a natural number q obtained by a natural number obtaining part 162, respectively. Thus, an output system suitable for outputting a PN series can be obtained.



LEGAL STATUS

[Date of request for examination]	31.05.1999
[Date of sending the examiner's decision of rejection]	
[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]	
[Date of final disposal for application]	
[Patent number]	3486133
[Date of registration]	24.10.2003
[Number of appeal against examiner's decision of rejection]	

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention] This invention relates to the output system which outputs PN (Pseudorandom Noise; pseudonoise) sequence, an output unit, an output method, and an information record medium. It is related with a suitable output system to output PN sequence which can be used as a diffusion sign of the CDMA (Code Division Multiple Access; code division multiple access) method of a spread spectrum system which can be especially used in the ranging fields, such as a land-mobile communication link of satellite communication, point to point communication, a cellular phone, PHS (Personal Handyphone System), etc., and GPS (Global Positioning System), an output unit, an output method, and an information record medium.
[0002]
[Description of the Prior Art] By using PN sequence as a diffusion sign, unknown episode nature is made high and the use effectiveness of a band is raised with the spread spectrum system using a CDMA method.
[0003] Conventionally, an M sequence, a Gold sign, ******, etc. were used as a PN sequence. Although it was calculable by combining a shift register, and this and an exclusive "or" circuit, since these sequences were based on a binary sequence, it was difficult for them to secure communication link security.
[0004] On the other hand, although it is necessary to take a synchronization in a spread spectrum system between the terminals which communicate, performing raising communication link security and a synchronization easily has the relation of a trade-off mutually.
[0005]
[Problem(s) to be Solved by the Invention] However, the technique of outputting PN sequence which can raise unknown episode nature further rather than PN sequence of these former is desired from the industrial world. Especially the request to the technique to which development outputs difficult PN sequence of identification, and raises the unknown episode nature of a spread spectrum system in recent years based on remarkable chaos theory, using this as a diffusion sign of a CDMA method is large.
[0006] On the other hand, in using PN sequence based on chaos theory simply, since the space which should search a diffusion sign becomes immense in case a synchronization is taken by the communicative receiving side, the technique of synchronizing easily is desired.
[0007] This invention was made in order to solve the above problems, and it aims at offering the output system which outputs PN sequence, an output unit, an output method, and an information record medium. It aims at offering a suitable output system outputting PN sequence which can be especially used as a diffusion sign of a spread spectrum system, an output unit, an output method, and an information record medium.
[0008]
[Means for Solving the Problem] In order to attain the above purpose, the following invention is indicated according to the principle of this invention.
[0009] elliptic function s (-) which set up the output system of PN sequence of this invention

beforehand The rational map F defined with the real number X (however, -1<X<1) and [a-17 number] (-, -) It is the output system of PN sequence which has the 1st and 2nd output units equipped with the natural number acquisition section based on the chevyshev map T (-, -) defined with [a-18 number], the transmitting value count section, the transmitting section, a receive section, the degree acquisition section, the initial value count section, and the sequence output section.

[0010] The natural number acquisition section of the 1st output unit is the natural number p. It acquires, the transmitting value count section calculates value Y=F (p, X), and the transmitting section is the value Y concerned. It transmits to the 2nd output unit.

[0011] The natural number acquisition section of the 2nd output unit is the natural number q. It acquires. A receive section Value Y which the 1st output unit transmitted It receives. The initial value count section Initial value Z=F (q, Y) is calculated. The degree acquisition section Degree s Acquiring, the sequence output section is the initial value Z concerned. Chevyshev map T (s, -) The PN sequences Z and T of the predetermined die length applied repeatedly (s, Z) T (s, T (s, Z)) and T (s, T (s, T (s, Z))), -- is outputted, the transmitting value count section calculates value Y'= F (q, X), and the transmitting section transmits the value Y' concerned to the 1st output unit.

[0012] The receive section of the 1st output unit receives value Y' which the 2nd output unit transmitted. The initial value count section Initial value Z'=F (p, Y') is calculated. The degree acquisition section Degree r Acquiring, the sequence output section is the chevyshev map T (r, -) to the initial value Z' concerned. PN sequence Z' of the predetermined die length applied repeatedly, T (r, Z'), T (r, T (r, Z')), and T (r, T (r, T (r, Z'))), It constitutes so that -- may be outputted.

[0013]

[Equation 17]

$$F(n, s(x)) = s(nx) \quad (n\text{は}2\text{以上の自然数})$$

[0014]

[Equation 18]

$$T(n, \cos x) = \cos nx \quad (n\text{は}2\text{以上の自然数})$$

[0015] Moreover, the degree which the degree acquisition section of the 1st and 2nd output units acquires can consist of output systems of PN sequence of this invention so that it may be the prime factor.

[0016] The output unit of PN sequence of this invention is elliptic function s (-) set up beforehand. It is the output unit of PN sequence based on the chevyshev map T (-, -) defined with the rational map F (-, -) defined with the real number X (however, -1<X<1) and [a-17 number], and [a-18 number].

[0017] This output unit is the natural number p. The natural number acquisition section to acquire and the transmitting value count section which calculates value Y=F (p, X), The value Y concerned With the transmitting section which transmits to the 2nd output unit, and the receive section which receives value Y' which the 2nd output unit transmitted The initial value count section which calculates initial value Z'=F (p, Y'), and degree r The degree acquisition section to acquire, It is the chevyshev map T (r, -) to the initial value Z' concerned. PN sequence Z' of the predetermined die length applied repeatedly, T (r, Z'), T (r, T (r, Z')), and T (r, T (r, T (r, Z'))), It constitutes so that it may have the sequence output section which outputs --.

[0018] Moreover, the degree which the degree acquisition section of the output unit of this invention acquires can be constituted so that it may be the prime factor.

[0019] The output system of PN sequence of this invention is elliptic function s (-) set up beforehand. It is the output system of PN sequence which has two or more output units based on the chevyshev map T (-, -) defined with the rational map F (-, -) defined with the real number X (however, -1<X<1) and [a-17 number], and [a-18 number].

[0020] Each of two or more output units which this output system has Natural number p The

natural number acquisition section to acquire and the transmitting value count section which calculates value Y=F (p, X), The value Y concerned With the transmitting section which transmits to other output units, and the receive section which receives value Y' which other output units transmitted When Function F (p, −) is not applied to the value Y' concerned yet, it is value Y"=F (p, Y'). The 2nd transmitting value count section to calculate, Concerned value Y" It is already Function F (p, −) to the 2nd transmitting section which transmits to other output units, and the value Y' concerned. The initial value count section which calculates initial value Z'=F (p, Y') when having applied, Degree r It is the chevyshev map T (r, −) to the degree acquisition section to acquire and the initial value Z' concerned. PN sequence Z' of the predetermined die length applied repeatedly, T (r, Z'), T (r, T (r, Z')) and T (r, T (r, T (r, Z'))), It constitutes so that it may have the sequence output section which outputs --.

[0021] Moreover, the degree which each natural number acquisition section of an output unit acquires can consist of output systems of this invention so that it may be the prime factor.

[0022] Moreover, the degree which the natural number acquisition section of the output unit which an output unit is classified into two or more groups, and belongs to the same group acquires can consist of output systems of this invention so that it may be the same natural number.

[0023] Moreover, an output unit is classified into two or more groups according to the output system of this invention, and the real number inputted into the transmitting value count section of the output unit belonging to the same group can consist of them so that it may be the same real number.

[0024] The output unit of PN sequence of this invention is elliptic function s (−) set up beforehand. It is the output unit of PN sequence based on the chevyshev map T (−, −) defined with the rational map F (−, −) defined with the real number X (however, −1<X<1) and [a−17 number], and [a−18 number].

[0025] This output unit is the natural number p. The natural number acquisition section to acquire and the natural number p concerned The transmitting value count section which calculates value Y=F (p, X) by being based, The value Y concerned With the transmitting section which transmits to other output units, and the receive section which receives value Y' which other output units transmitted When Function F (p, −) is not applied to the value Y' concerned yet, it is value Y"=F (p, Y'). The 2nd transmitting value count section to calculate, Concerned value Y" The 2nd transmitting section which transmits to other output units, and the initial value count section which calculates initial value Z'=F (p, Y') based on the natural number q concerned and the value Y' concerned when Function F (p, −) is already applied to the value Y' concerned, Degree r It is the chevyshev map T (r, −) to the degree acquisition section to acquire and the initial value Z' concerned. PN sequence Z' of the predetermined die length applied repeatedly, T (r, Z'), T (r, T (r, Z')) and T (r, T (r, T (r, Z'))), It constitutes so that it may have the sequence output section which outputs --.

[0026] Moreover, the degree which the degree acquisition section of the output unit of this invention acquires can be constituted so that it may be the prime factor.

[0027] The output method of PN sequence of this invention is elliptic function s (−) set up beforehand. It is the output method of PN sequence based on the chevyshev map T (−, −) defined with the rational map F (−, −) defined with the real number X (however, −1<X<1) and [a−17 number], and [a−18 number].

[0028] This output method is the natural number p. The natural number acquisition procedure to acquire and the transmitting value computational procedure which calculates value Y=F (p, X), The value Y concerned The transmitting procedure transmitted to the 2nd output unit, and the receiving procedure of receiving value Y' which the 2nd output unit transmitted, The initial value computational procedure which calculates initial value Z'=F (p, Y'), and degree r The degree acquisition procedure to acquire, It is the chevyshev map T (r, −) to the initial value Z' concerned. PN sequence Z' of the predetermined die length applied repeatedly, T (r, Z'), T (r, T (r, Z')), and T (r, T (r, T (r, Z'))), It constitutes so that it may have the sequence output procedure which outputs --.

[0029] Moreover, the degree acquired in the degree acquisition procedure of the output method

of this invention can be constituted so that it may be the prime factor.
[0030] The output method of PN sequence of this invention is elliptic function s (-) set up beforehand. It is the output method of PN sequence based on the chevyshev map T (-, -) defined with the rational map F (-, -) defined with the real number X (however, -1<X<1) and [a-17 number], and [a-18 number].
[0031] This output method is the natural number p. The natural number acquisition procedure to acquire and the natural number p concerned The transmitting value computational procedure which calculates value Y=F (p, X) by being based, The value Y concerned The transmitting procedure transmitted to other output units, and the receiving procedure of receiving value Y' which other output units transmitted, When Function F (p, -) is not applied to the value Y' concerned yet, it is value Y"=F (p, Y'). The 2nd transmitting value computational procedure to calculate, Concerned value Y" The 2nd transmitting procedure which transmits to other output units, and the initial value computational procedure which calculates initial value Z'=F (p, Y') based on the natural number q concerned and the value Y' concerned when Function F (p, -) is already applied to the value Y' concerned, Degree r It is the chevyshev map T (r, -) to the degree acquisition procedure to acquire and the initial value Z' concerned. PN sequence Z' of the predetermined die length applied repeatedly, T (r, Z'), T (r, T (r, Z')) and T (r, T (r, T (r, Z'))), It constitutes so that it may have the sequence output procedure which outputs --.
[0032] Moreover, the degree acquired in the degree acquisition procedure of the output method of this invention can be constituted so that it may be the prime factor.
[0033] The program which realizes the output system of PN sequence of this invention, an output unit, and an output method is recordable on information record media, such as a compact disk, a floppy disk, a hard disk, a magneto-optic disk, a digital video disc, a magnetic tape, and semiconductor memory.
[0034] The output system of the above-mentioned PN sequence, an output unit, and an output method are realizable by performing the program recorded on the information record medium of this invention with information processors equipped with storage, count equipment, an output unit, etc., such as a general purpose computer and a parallel computer.
[0035] Moreover, with an information processor, the information record medium which recorded the program of this invention can be distributed and sold independently.
[0036]
[Embodiment of the Invention] One operation gestalt of this invention is explained below. In addition, the operation gestalt explained below is a thing for explanation, and does not restrict the range of the invention in this application. Therefore, although it is possible to adopt the operation gestalt which permuted each of these elements or all elements by this and the equal thing if it is this contractor, these operation gestalten are also included in the range of the invention in this application.
[0037] (Gestalt of the 1st operation) Drawing 1 is the mimetic diagram (data flow diagram) showing the output structure of a system of PN sequence of this invention. In addition, drawing 1 can also be seen as a flow chart performed in order of the arrow head of the vertical direction. Hereafter, it explains with reference to drawing 1 .
[0038] The output system 101 has an output unit 111 and an output unit 161.
[0039] An output unit 111 is equipped with the natural number acquisition section 112, the transmitting value count section 113, the transmitting section 114, a receive section 115, the initial value count section 116, the degree acquisition section 117, and the sequence output section 118.
[0040] On the other hand, an output unit 161 is equipped with the natural number acquisition section 162, the transmitting value count section 163, the transmitting section 164, a receive section 165, the initial value count section 166, the degree acquisition section 167, and the sequence output section 168.
[0041] The natural number acquisition section 112 of an output unit 111, the natural number acquisition section 162 of an output unit 161, and ** and the respectively to some extent big natural number p Natural number q It acquires. These natural numbers function as a private key.
[0042] Elliptic function s beforehand set up between the output unit 111 and the output unit 161

(-) The public key X of the real number which carried out predetermined quality assurance (- 1< X<1) is shared. Here, it is elliptic function s (-). Public key X Even if monitored, communication link security does not fall so that it may mention later.
[0043] the transmitting value count section 113 of an output unit 111, the transmitting value count section 163 of an output unit 161, and ** and the natural number p which the natural number acquisition section 112 acquired, respectively The natural number q which the natural number acquisition section 162 acquired from -- respectively -- value Y=F (p, X) and value Y'=F (q, X) It calculates.
[0044] Here, Map F (-, -) is a rational map defined by the elliptic function, and a rational polynomial can express it directly. That is, it is easily realizable with association of the electronic circuitry which performs the transmitting value count section 113, the transmitting value count section 163, and ** and four operations, CPU (Central Processing Unit; central-process unit) of a computer, memory, etc., etc.
[0045] It is a value Y to the transmitting section 114 of an output unit 111, the transmitting section 164 of an output unit 161, each ** and the receive section 165 of an output unit 161, and the receive section 115 of an output unit 111. Value Y' is transmitted. Value Y Even if value Y' is monitored, communication link security does not fall so that it may mention later.
[0046] The initial value count section 116 of an output unit 111, the initial value count section 166 of an output unit 161, ** and value Y' which the receive section 115 of an output unit 111, the receive section 165 of an output unit 161, and ** received, respectively, and value Y Initial value Z'=F (p, Y') and initial value Z=F (q, Y) are calculated by being based.
[0047] Here, the rational map F (-, -) is elliptic function s (-). Since it is defined by the addition theorem, the following properties are materialized.
Z'=F(p, Y') =F(p, F (q, X)) =F(q, F (p, X)) =F(q, Y) =Z' [0048] Thus, the initial value of the diffusion sign of an output unit 111, an output unit 161, and a ** and a CDMA method is sharable.
[0049] The degree acquisition section 117 of an output unit 111, the degree acquisition section 167 of an output unit 161, and each ** and Degree r Degree s It acquires. Degrees are the two or more natural numbers, and it is desirable that it is the prime factor.
[0050] The sequence output section 118 of an output unit 111, the sequence output section 168 of an output unit 161, and **, respectively -- chevyshev map T (r, -) Chevyshev map T (s, -) The PN sequences Z and T of the predetermined die length of the following repeatedly applied to value Z=Z' (r, Z) T (r, T (r, Z)) and T (r, T (r, T (r, Z))) -- Z, T (s, Z), T (s, T (s, Z)), and T (s, T (s, T (s, Z))), -- is outputted. This PN sequence can be outputted by the repeat count by the recurrence formula.
[0051] The example of a chevyshev map is shown in drawing 2 . In drawing 2 , it is [the chevyshev map T (2 -), T (3 -), and T of degrees 2-5 (4 -), and] T (5 -). Graphical representation is carried out. Although a chevyshev map is a rational map which maps the section (- 1 one) at the section (- 1 one) and the addition theorem of a cosine function can define it, it can also be directly expressed by the rational polynomial. [The-20 number of [a-19 number]] of a degree 2 is the polynomial representation of a chevyshev map of a degree 3.
[0052]
[Equation 19]
$$T(2,y) = 2y^2 - 1$$

[0053]
[Equation 20]
$$T(3,y) = 4y^3 - 3y$$

[0054] Therefore, it is easily realizable with association of the electronic circuitry which performs the sequence output section 118, the sequence output section 168, and ** and four operations, CPU of a computer, memory, etc., etc.
[0055] When these PN sequences are used as a diffusion sign of a CDMA method, a correlation function intersects perpendicularly mostly. That a correlation property is good as compared with

the conventional M sequence, a Gold sign, and ****** By artificers It is discovered (). [K.Umeno and] K.Kitayama and Electoronics Letters (1999) Vol. 35 pp.545-546 ; K.Umeno and K.Kitayama, to appear in Proc.1999 IEEE Information Theory Workshop.
[0056] Then, according to ** and PN sequence of the above respectively, spectrum diffusion is performed and it communicates with a communication device (not shown) equipped with an output unit 111, and a communication device (not shown) equipped with an output unit 161.
[0057] A communication device equipped with an output unit 111, a communication device equipped with an output unit 161, **, and the signal in which spectrum diffusion was carried out by PN sequence of the above respectively will be received. In this case, although the synchronization of a CDMA method is needed, since the degrees of a chevyshev map only differ, the above-mentioned PN sequence can narrow search space of a synchronization. Moreover, since the correlation property of the diffusion sign generated by these Chebyshev polynominals lies at right angles in the sense of a correlation function, it can take a synchronization easily by performing correlation detection etc.
[0058] on the other hand -- elliptic function s (-) a public key X, a value Y, value Y', and ** .-- even if information [like] is monitored, the others guess initial value Z=Z' of PN sequence, and the PN sequence itself -- ellipse Diffe-Hellman It becomes a problem and an equivalent problem. It is known that solving is very difficult for this problem (N. KOBURITTSU, a Koichi Sakurai translation, a number theory algorithm, a guide to elliptic curve cryptosystem theoretical, Springer-Verlag Tokyo, and 1997).
[0059] While making communication link security by this higher than the diffusion sign used by the existing CDMA method by the diffusion sign using chaos, two purposes of making a synchronization easy can be attained.
[0060] Here, it is a public key X. Since initial value also serves as a rational number when carrying out and using a rational number, the initial value which the output unit 111 and the output unit 161 calculated is strictly in agreement (Z=Z'). On the other hand, it is a public key X. Initial value can be made in agreement, if it maintains a sufficiently high precision in carrying out and using a floating point number etc. in this case, public key X from -- initial value Z=Z' shared is processed as digital information.
[0061] In addition, the output unit 111 of this invention, an output unit 161, and ** and all can be divided into the communications department (the transmitting section 114, a receive section 115 and the transmitting section 164, receive section 165) which transmits and receives, and the part which performs the other processing.
[0062] Among these, parts other than the communications department can be constituted by the electronic circuitry which performs four operations etc., and can be mounted as a unified chip. Moreover, parts other than the communications department can also be mounted by computer which has CPU and memory. If these are these contractors, it can mount easily with a well-known technique, and these operation gestalten are included in the range of this invention.
[0063] (Gestalt of the 2nd operation) Although the 1st operation gestalt outputted the diffusion sign which can be used in the spread spectrum system of the CDMA method of 1 to 1 by chaos, this operation gestalt can be applied when three or more users communicate mutually especially, two or more users and.
[0064] Drawing 3 is the mimetic diagram (data flow diagram) showing the outline of the output unit used by the output system of this operation gestalt. In addition, drawing 3 can also be seen as a flow chart performed in order of the arrow head of the vertical direction.
[0065] The output unit 311 of this operation gestalt is equipped with the natural number acquisition section 312, the transmitting value count section 313, the transmitting section 314, a receive section 315, the initial value count section 316, the degree acquisition section 317, the sequence output section 318, the 2nd transmitting value count section 320, and the 2nd transmitting section 321.
[0066] The natural number acquisition section 312 of an output unit 311 is the to some extent big natural number p. It acquires. This natural number functions as a private key.
[0067] Elliptic function s beforehand set up between the output units 311 which communicate mutually within a system (-) The public key X of the real number which carried out

predetermined quality assurance (- 1< X<1) is shared.
[0068] the natural number p from which the natural number acquisition section 312 acquired the transmitting value count section 313 of an output unit 311 from -- value Y=F (p, X) is calculated.

[0069] The transmitting section 314 of an output unit 311 is a value Y to the receive section 315 of other output units 311. It transmits.
[0070] When the receive section 315 of an output unit 311 receives value Y' transmitted from other output units 311, self is also already Map F (p, -) to the value Y' concerned. It distinguishes whether it has applied and other output units 311 have applied each map.
[0071] When having not applied yet, the 2nd transmitting value count section 320 is value Y"=F (p, Y'). Calculating, the 2nd transmitting section 321 is concerned value Y". It transmits to other output units 311. In addition, it is realizable, using the hardware with the 2nd same transmitting section 321 and transmitting section 314 in common.
[0072] When having already applied, the initial value count section 316 of an output unit 311 calculates initial value Z'=F (p, Y').
[0073] In addition, this distinction is Y about the information which identifies the output unit which applied the map. Y" It can double, can communicate mutually and can carry out by examining this information.
[0074] Moreover, for this distinction, the number of users is K. When it is people (K>=3), as shown in drawing 4 , it can carry out by forming a counter 319. In drawing 4 , illustration is omitted about the part which gives the same sign to drawing 3 and a common element, and does not have a difference. A counter 319 is first cleared by 0, and whenever a receive section 315 receives the value transmitted from other output units 311, the increment of it is carried out every [1].
[0075] When the value by which counting is carried out is expressed in a counter 319 as K', in the case of K'<K-2, there will be some which have not applied the map yet among other output units 311. In this case, since it is not what made it the origin for Y' to have been transmitted by the transmitting section 314 of other output units 311, and was transmitted from the own transmitting section 314, it is the own map F (p, -) by the 2nd transmitting value count section 320. It applies.
[0076] In the case of K'=K-2, self will also already have applied the map and other output units 311 will have applied each map. In this case, the value of a counter 319 is cleared to 0 and initial value is made to calculate by the initial value count section 316.
[0077] Here, the rational map F (-, -) is a certain specific elliptic function s (-). Since it is defined by the addition theorem, if the map by the 2nd transmitting value count section 320 of all the output units 311 is applied, initial value Z' will become the same value with all output units.
[0078] For this, in for example, 3 person communication links, the natural number acquisition section of three output units 311 is p, q, and t, respectively. Supposing it acquires, it is because the following properties are materialized.
F () [p,] [F]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1] Elliptic function s set up beforehand (-) Real number X (however, -1<X<1) The natural number acquisition section based on the chevyshev map T (-, -) defined with the rational map F (-, -) defined with [a-one number], and [a-two number], The transmitting value count section, the transmitting section, a receive section, the degree acquisition section, and the initial value count section, It is the output system of the pseudonoise sequence which has the 1st and 2nd output units equipped with the sequence output section. The natural number acquisition section of said 1st output unit Natural number p It acquires and the transmitting value count section calculates value Y=F (p, X). The transmitting section The value Y concerned It transmits to said 2nd output unit. The natural number acquisition section of said 2nd output unit Natural number q It is the value Y to which it acquired and said 1st output unit transmitted the receive section. It receives. The initial value count section Initial value Z=F (q, Y) is calculated. The degree acquisition section Degree s Acquiring, the sequence output section is the initial value Z concerned. Chevyshev map T (s, -) The pseudonoise sequences Z and T of the predetermined die length applied repeatedly (s, Z) T (s, T (s, Z)) and T (s, T (s, T (s, Z))), -- is outputted. The transmitting value count section Value Y'=F (q, X) It calculates. The transmitting section The value Y' concerned is transmitted to said 1st output unit. The receive section of said 1st output unit Value Y' which said 2nd output unit transmitted is received. The initial value count section Initial value Z'=F (p, Y') is calculated. The degree acquisition section Degree r Acquiring, the sequence output section is the chevyshev map T (r, -) to the initial value Z' concerned. Pseudonoise sequence Z' of the predetermined die length applied repeatedly, T (r, Z'), T (r, T (r, Z')) and T (r, T (r, T (r, Z'))), Output system characterized by outputting --.
[Equation 1]
$F(n, s(x)) = s(nx)$ (nは2以上の自然数)

[Equation 2]
$T(n, \cos x) = \cos nx$ (nは2以上の自然数)

[Claim 2] The degree which the degree acquisition section of said 1st and 2nd output units acquires is an output system according to claim 1 characterized by being the prime factor.
[Claim 3] Elliptic function s set up beforehand (-) Real number X (however, -1<X<1) It is the output unit of the pseudonoise sequence based on the chevyshev map T (-, -) defined with the rational map F (-, -) defined with [a-three number], and [a-four number], and is the natural number p. The natural number acquisition section to acquire, The transmitting value count section which calculates value Y=F (p, X), and the value Y concerned The transmitting section which transmits to the 2nd output unit, The receive section which receives value Y' which said 2nd output unit transmitted, and the initial value count section which calculates initial value Z'=F (p, Y'), Degree r It is the chevyshev map T (r, -) to the degree acquisition section to acquire and the initial value Z' concerned. Pseudonoise sequence Z' of the predetermined die length applied repeatedly, T (r, Z'), T (r, T (r, Z')) and T (r, T (r, T (r, Z'))), Output unit characterized by having the sequence output section which outputs --.

[Equation 3]
$F(n, s(x)) = s(nx)$ (nは２以上の自然数)

[Equation 4]
$T(n, \cos x) = \cos nx$ (nは２以上の自然数)

[Claim 4] The degree which said degree acquisition section acquires is an output unit according to claim 3 characterized by being the prime factor.
[Claim 5] Elliptic function s set up beforehand (-) Real number X (however, -1<X<1) It is the output system of the pseudonoise sequence which has two or more output units based on the chevyshev map T (-, -) defined with the rational map F (-, -) defined with [a-five number], and [a-six number]. Each of said output unit is the natural number p. The natural number acquisition section to acquire, The transmitting value count section which calculates value Y=F (p, X), and the value Y concerned The transmitting section which transmits to other output units, It is still Function F (p, -) to the receive section which receives value Y' which the output unit which is others transmitted, and the value Y' concerned. When having not applied, it is value Y"=F (p, Y'). The 2nd transmitting value count section to calculate, Concerned value Y" It is already Function F (p, -) to the 2nd transmitting section which transmits to other output units, and the value Y' concerned. The initial value count section which calculates initial value Z'=F (p, Y') when having applied, Degree r It is the chevyshev map T (r, -) to the degree acquisition section to acquire and the initial value Z' concerned. Pseudonoise sequence Z' of the predetermined die length applied repeatedly, T (r, Z'), T (r, T (r, Z')) and T (r, T (r, T (r, Z'))), Output system characterized by having the sequence output section which outputs --.
[Equation 5]
$F(n, s(x)) = s(nx)$ (nは２以上の自然数)

[Equation 6]
$T(n, \cos x) = \cos nx$ (nは２以上の自然数)

[Claim 6] The degree which each natural number acquisition section of said output unit acquires is an output system according to claim 5 characterized by being the prime factor.
[Claim 7] The real number inputted into the transmitting value count section of the output unit which said output system is classified into two or more groups, and belongs to the same group is an output system according to claim 5 or 6 characterized by being the same real number.
[Claim 8] Elliptic function s set up beforehand (-) Real number X (however, -1<X<1) It is the output unit of the pseudonoise sequence based on the chevyshev map T (-, -) defined with the rational map F (-, -) defined with [a-seven number], and [a-eight number], and is the natural number p. The natural number acquisition section to acquire, The natural number p concerned The transmitting value count section which calculates value Y=F (p, X) by being based, The value Y concerned With the transmitting section which transmits to other output units, and the receive section which receives value Y' which other output units transmitted When Function F (p, -) is not applied to the value Y' concerned yet, it is value Y"=F (p, Y'). The 2nd transmitting value count section to calculate, Concerned value Y" The 2nd transmitting section which transmits to other output units, and the initial value count section which calculates initial value Z'=F (p, Y') based on the natural number p concerned and the value Y' concerned when Function F (p, -) is already applied to the value Y' concerned, Degree r It is the chevyshev map T (r, -) to the degree acquisition section to acquire and the initial value Z' concerned. Pseudonoise sequence Z' of the predetermined die length applied repeatedly, T (r, Z'), T (r, T (r, Z')) and T (r, T (r, T (r, Z'))), Output unit characterized by having the sequence output section which outputs --.
[Equation 7]
$F(n, s(x)) = s(nx)$ (nは２以上の自然数)

[Equation 8]

$T(n, \cos x) = \cos nx$ （nは２以上の自然数）

[Claim 9] The degree which the degree acquisition section of said output unit acquires is an output unit according to claim 8 characterized by being the prime factor.
[Claim 10] Elliptic function s set up beforehand (-) Real number X (however, -1<X<1) It is the output method of the pseudonoise sequence based on the chevyshev map T (-, -) defined with the rational map F (-, -) defined with [a-nine number], and [a-ten number], and is the natural number p. The natural number acquisition procedure to acquire, The transmitting value computational procedure which calculates value Y=F (p, X), and the value Y concerned The transmitting procedure transmitted to the 2nd output unit, The receiving procedure of receiving value Y' which said 2nd output unit transmitted, and the initial value computational procedure which calculates initial value Z'=F (p, Y'), Degree r It is the chevyshev map T (r, -) to the degree acquisition procedure to acquire and the initial value Z' concerned. Pseudonoise sequence Z' of the predetermined die length applied repeatedly, T (r, Z'), T (r, T (r, Z')) and T (r, T (r, T (r, Z')))), Output method characterized by having the sequence output procedure which outputs --.
[Equation 9]
$F(n, s(x)) = s(nx)$ （nは２以上の自然数）

[Equation 10]
$T(n, \cos x) = \cos nx$ （nは２以上の自然数）

[Claim 11] The degree acquired in said degree acquisition procedure is an output method according to claim 10 characterized by being the prime factor.
[Claim 12] Elliptic function s set up beforehand (-) Real number X (however, -1<X<1) It is the output method of the pseudonoise sequence based on the chevyshev map T (-, -) defined with the rational map F (-, -) defined with [a-11 number], and [a-12 number], and is the natural number p. The natural number acquisition procedure to acquire, The natural number p concerned The transmitting value computational procedure which calculates value Y=F (p, X) by being based, The value Y concerned The transmitting procedure transmitted to other output units, and the receiving procedure of receiving value Y' which other output units transmitted, When Function F (p, -) is not applied to the value Y' concerned yet, it is value Y''=F (p, Y'). The 2nd transmitting value computational procedure to calculate, Concerned value Y'' The 2nd transmitting procedure which transmits to other output units, and the initial value computational procedure which calculates initial value Z'=F (p, Y') based on the natural number q concerned and the value Y' concerned when Function F (p, -) is already applied to the value Y' concerned, Degree r It is the chevyshev map T (r, -) to the degree acquisition procedure to acquire and the initial value Z' concerned. Pseudonoise sequence Z' of the predetermined die length applied repeatedly, T (r, Z'), T (r, T (r, Z')) and T (r, T (r, T (r, Z')))), Output method characterized by having the sequence output procedure which outputs --.
[Equation 11]
$F(n, s(x)) = s(nx)$ （nは２以上の自然数）

[Equation 12]
$T(n, \cos x) = \cos nx$ （nは２以上の自然数）

[Claim 13] The degree acquired in said degree acquisition procedure is an output method according to claim 12 characterized by being the prime factor.
[Claim 14] Elliptic function s set up beforehand (-) Real number X (however, -1<X<1) It is the information record medium which recorded the program which realizes processing which outputs the pseudonoise sequence based on the chevyshev map T (-, -) defined with the rational map F (-, -) defined with [a-13 number], and [a-14 number] and in which computer reading is possible. Natural number p The natural number acquisition procedure to acquire and the transmitting value computational procedure which calculates value Y=F (p, X), The value Y concerned The

transmitting procedure transmitted to the 2nd output unit, and the receiving procedure of receiving value Y' which said 2nd output unit transmitted, The initial value computational procedure which calculates initial value Z'=F (p, Y'), and degree r The degree acquisition procedure to acquire, It is the chevyshev map T (r, -) to the initial value Z' concerned. Pseudonoise sequence Z' of the predetermined die length applied repeatedly, T (r, Z'), T (r, T (r, Z')) and T (r, T (r, T (r, Z')))), Information record medium characterized by recording the program which realizes processing equipped with the sequence output procedure which outputs --.

[Equation 13]

$$F(n, s(x)) = s(nx) \quad (n \text{は} 2 \text{以上の自然数})$$

[Equation 14]

$$T(n, \cos x) = \cos nx \quad (n \text{は} 2 \text{以上の自然数})$$

[Claim 15] The degree acquired in said degree acquisition procedure is an information record medium according to claim 14 characterized by being the prime factor.

[Claim 16] Elliptic function s set up beforehand (-) Real number X (however, -1<X<1) It is the information record medium which recorded the program which realizes processing which outputs the pseudonoise sequence based on the chevyshev map T (-, -) defined with the rational map F (-, -) defined with [a-15 number], and [a-16 number] and in which computer reading is possible. Natural number p The natural number acquisition procedure to acquire and the natural number p concerned The transmitting value computational procedure which calculates value Y=F (p, X) by being based, The value Y concerned The transmitting procedure transmitted to other output units, and the receiving procedure of receiving value Y' which other output units transmitted, When Function F (p, -) is not applied to the value Y' concerned yet, it is value Y''=F (p, Y'). The 2nd transmitting value computational procedure to calculate, Concerned value Y'' The 2nd transmitting procedure which transmits to other output units, and the initial value computational procedure which calculates initial value Z'=F (p, Y') based on the natural number q concerned and the value Y' concerned when Function F (p, -) is already applied to the value Y' concerned, Degree r It is the chevyshev map T (r, -) to the degree acquisition procedure to acquire and the initial value Z' concerned. Pseudonoise sequence Z' of the predetermined die length applied repeatedly, T (r, Z'), T (r, T (r, Z')) and T (r, T (r, T (r, Z')))), Information record medium characterized by recording the program which realizes processing equipped with the sequence output procedure which outputs --.

[Equation 15]

$$F(n, s(x)) = s(nx) \quad (n \text{は} 2 \text{以上の自然数})$$

[Equation 16]

$$T(n, \cos x) = \cos nx \quad (n \text{は} 2 \text{以上の自然数})$$

[Claim 17] The degree acquired in said degree acquisition procedure is an information record medium according to claim 16 characterized by being the prime factor.

[Claim 18] Said information record medium is a compact disk, a floppy (trademark) disk, a hard disk, a magneto-optic disk, a digital video disc, a magnetic tape, or an information record medium given in 16 from claim 14 characterized by being semiconductor memory.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1] It is the mimetic diagram showing the configuration of the 1st of the gestalt of operation of the output system of PN sequence of this invention.
[Drawing 2] It is the graph which shows the situation of a chevyshev map.
[Drawing 3] It is the mimetic diagram showing the configuration of the 2nd of the gestalt of operation of the output system of PN sequence of this invention.
[Drawing 4] It is the mimetic diagram showing the configuration of the 2nd of the counter of the gestalt of operation etc. of the output system of PN sequence of this invention.
[Description of Notations]
101 Output System
111 1st Output Unit
112 Natural Number Acquisition Section
113 Transmitting Value Count Section
114 Transmitting Section
115 Receive Section
116 Initial Value Count Section
117 Degree Acquisition Section
118 Sequence Output Section
161 2nd Output Unit
162 Natural Number Acquisition Section
163 Transmitting Value Count Section
164 Transmitting Section
165 Receive Section
166 Initial Value Count Section
167 Degree Acquisition Section
168 Sequence Output Section
311 Output Unit
312 Natural Number Acquisition Section
313 Transmitting Value Count Section
314 Transmitting Section
315 Receive Section
316 Initial Value Count Section
317 Degree Acquisition Section
318 Sequence Output Section
319 Counter
320 2nd Transmitting Value Count Section
321 2nd Transmitting Section

[Translation done.]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号
特開2000－338869
（P2000－338869A）
(43)公開日　平成12年12月８日(2000.12.8)

(51)Int.Cl.[7]	識別記号	ＦＩ		テーマコード*（参考）
Ｇ０９Ｃ　1/00	６５０	Ｇ０９Ｃ　1/00	６５０Ｂ	５Ｊ１０４
Ｈ０４Ｊ　13/00		Ｈ０４Ｊ　13/00	Ａ	５Ｋ０２２

審査請求　有　　請求項の数18　ＯＬ　（全 11 頁）

(21)出願番号　特願平11－152063

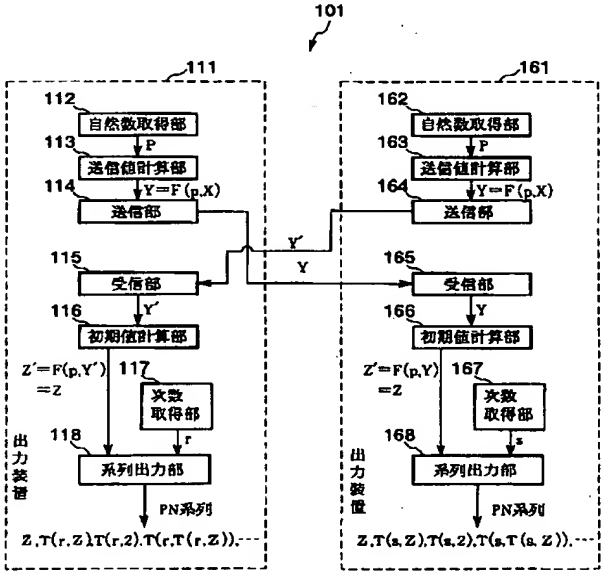
(22)出願日　平成11年５月31日(1999.5.31)

(71)出願人　391027413
郵政省通信総合研究所長
東京都小金井市貫井北町４丁目２番１号
(71)出願人　597044841
梅野　健
東京都小金井市貫井北町４丁目２番地１号
郵政省通信総合研究所内
(72)発明者　梅野　健
東京都小金井市貫井北町４丁目２番１号
郵政省通信総合研究所内
(74)代理人　100095407
弁理士　木村　満　（外１名）

Ｆターム(参考)　5J104 AA01 FA00 NA04 PA01
5K022 EE02 EE25 EE36

(54)【発明の名称】　擬似雑音系列の出力システム、出力装置、出力方法、および、情報記録媒体

(57)【要約】
【課題】　擬似雑音系列の出力システム、出力装置、出力方法、情報記録媒体を提供する。
【解決手段】　擬似雑音系列の出力システムの複数の出力装置のそれぞれは、自然数p を取得する自然数取得部と、値Y=F(p,X)を計算する送信値計算部と、当該値Y を他の出力装置に送信する送信部と、他の出力装置が送信した値Y'を受信する受信部と、当該値Y'にまだ関数F(p,・) を適用していない場合、値Y''=F(p,Y') を計算する第２の送信値計算部と、当該値Y'' を他の出力装置に送信する第２の送信部と、当該値Y'に既に関数F(p,・) を適用している場合、初期値Z'=F(p,Y')を計算する初期値計算部と、次数r を取得する次数取得部と、当該初期値Z'にチェビシェフ写像T(r,・) を繰り返し適用した所定の長さの系列Z', T(r,Z'),T(r,T(r,Z')), T(r,T(r,T(r,Z'))), …を出力する系列出力部と、を備える。



【特許請求の範囲】

【請求項１】あらかじめ設定した楕円関数s(・) と、実数X (ただし-1<;X<;1)と、［数１］により定義される有理写像F(・,・)と、［数２］により定義されるチェビシェフ写像T(・,・)とに基づいた、自然数取得部と、送信値計算部と、送信部と、受信部と、次数取得部と、初期値計算部と、系列出力部とを備える第１および第２の出力装置を有する擬似雑音系列の出力システムであって、

前記第１の出力装置の自然数取得部は、自然数p を取得し、送信値計算部は、値Y=F(p, X)を計算し、送信部は、当該値Y を前記第２の出力装置に送信し、

前記第２の出力装置の自然数取得部は、自然数q を取得し、受信部は、前記第１の出力装置が送信した値Y を受信し、初期値計算部は、初期値Z=F(q, Y)を計算し、次数取得部は、次数s を取得し、系列出力部は、当該初期値Z にチェビシェフ写像T(s, ・) を繰り返し適用した所定の長さの擬似雑音系列

Z, T(s, Z), T(s, T(s, Z)), T(s, T(s, T(s, Z))), …

を出力し、送信値計算部は、値Y'=F(q, X) を計算し、送信部は、当該値Y' を前記第１の出力装置に送信し、

前記第１の出力装置の受信部は、前記第２の出力装置が送信した値Y' を受信し、初期値計算部は、初期値Z'=F(p, Y')を計算し、次数取得部は、次数r を取得し、系列出力部は、当該初期値Z' にチェビシェフ写像T(r, ・) を繰り返し適用した所定の長さの擬似雑音系列

Z', T(r, Z'), T(r, T(r, Z')), T(r, T(r, T(r, Z'))), …

を出力することを特徴とする出力システム。

【数１】

$$F(n, s(x)) = s(nx) \quad (n\text{は２以上の自然数})$$

【数２】

$$T(n, \cos x) = \cos nx \quad (n\text{は２以上の自然数})$$

【請求項２】前記第１および第２の出力装置の次数取得部が取得する次数は、素数であることを特徴とする請求項１記載の出力システム。

【請求項３】あらかじめ設定した楕円関数s(・) と、実数X (ただし-1<;X<;1)と、［数３］により定義される有理写像F(・,・)と、［数４］により定義されるチェビシェフ写像T(・,・)とに基づいた擬似雑音系列の出力装置であって、

自然数p を取得する自然数取得部と、

値Y=F(p, X)を計算する送信値計算部と、

当該値Y を第２の出力装置に送信する送信部と、

前記第２の出力装置が送信した値Y' を受信する受信部と、

初期値Z'=F(p, Y')を計算する初期値計算部と、

次数r を取得する次数取得部と、

当該初期値Z' にチェビシェフ写像T(r, ・) を繰り返し適用した所定の長さの擬似雑音系列

Z', T(r, Z'), T(r, T(r, Z')), T(r, T(r, T(r, Z'))), …

を出力する系列出力部と、

を備えることを特徴とする出力装置。

【数３】

$$F(n, s(x)) = s(nx) \quad (n\text{は２以上の自然数})$$

【数４】

$$T(n, \cos x) = \cos nx \quad (n\text{は２以上の自然数})$$

【請求項４】前記次数取得部が取得する次数は、素数であることを特徴とする請求項３記載の出力装置。

【請求項５】あらかじめ設定した楕円関数s(・) と、実数X (ただし-1<;X<;1)と、［数５］により定義される有理写像F(・,・)と、［数６］により定義されるチェビシェフ写像T(・,・)とに基づいた複数の出力装置を有する擬似雑音系列の出力システムであって、

前記出力装置のそれぞれは、

自然数p を取得する自然数取得部と、

値Y=F(p, X)を計算する送信値計算部と、

当該値Y を他の出力装置に送信する送信部と、

他の出力装置が送信した値Y' を受信する受信部と、

当該値Y' にまだ関数F(p, ・) を適用していない場合、値Y''=F(p, Y') を計算する第２の送信値計算部と、

当該値Y'' を他の出力装置に送信する第２の送信部と、

当該値Y' に既に関数F(p, ・) を適用している場合、初期値Z'=F(p, Y')を計算する初期値計算部と、

次数r を取得する次数取得部と、

当該初期値Z' にチェビシェフ写像T(r, ・) を繰り返し適用した所定の長さの擬似雑音系列

Z', T(r, Z'), T(r, T(r, Z')), T(r, T(r, T(r, Z'))), …

を出力する系列出力部と、

を備えることを特徴とする出力システム。

【数５】

$$F(n, s(x)) = s(nx) \quad (n\text{は２以上の自然数})$$

【数６】

$$T(n, \cos x) = \cos nx \quad (n\text{は２以上の自然数})$$

【請求項６】前記出力装置のそれぞれの自然数取得部が取得する次数は、素数であることを特徴とする請求項５記載の出力システム。

【請求項７】前記出力システムは複数の群に分類され、同じ群に属する出力装置の送信値計算部に入力される実数は、同じ実数であることを特徴とする請求項５または６記載の出力システム。

【請求項８】あらかじめ設定した楕円関数s(・) と、実数X（ただし-1<;X<;1)と、［数７］により定義される有理写像F(・, ・)と、［数８］により定義されるチェビシェフ写像T(・, ・)とに基づいた擬似雑音系列の出力装置であって、

自然数p を取得する自然数取得部と、

当該自然数p に基づいて値Y=F(p, X)を計算する送信値計算部と、

当該値Y を他の出力装置に送信する送信部と、

他の出力装置が送信した値Y' を受信する受信部と、

当該値Y' にまだ関数F(p, ・) を適用していない場合、値Y' ' =F(p, Y') を計算する第２の送信値計算部と、

当該値Y' ' を他の出力装置に送信する第２の送信部と、

当該値Y' に既に関数F(p, ・) を適用している場合、当該自然数p と当該値Y' に基いて初期値Z' =F(p, Y') を計算する初期値計算部と、

次数r を取得する次数取得部と、

当該初期値Z' にチェビシェフ写像T(r, ・) を繰り返し適用した所定の長さの擬似雑音系列

Z', T(r, Z'), T(r, T(r, Z')), T(r, T(r, T(r, Z'))), …

を出力する系列出力部と、

を備えることを特徴とする出力装置。

【数７】

$$F(n, s(x)) = s(nx) \quad (n\text{は２以上の自然数})$$

【数８】

$$T(n, \cos x) = \cos nx \quad (n\text{は２以上の自然数})$$

【請求項９】前記出力装置の次数取得部が取得する次数は、素数であることを特徴とする請求項８記載の出力装置。

【請求項１０】あらかじめ設定した楕円関数s(・) と、実数X（ただし-1<;X<;1)と、［数９］により定義される有理写像F(・, ・)と、［数１０］により定義されるチェビシェフ写像T(・, ・)とに基づいた擬似雑音系列の出力方法であって、

自然数p を取得する自然数取得手順と、

値Y=F(p, X)を計算する送信値計算手順と、

当該値Y を第２の出力装置に送信する送信手順と、

前記第２の出力装置が送信した値Y' を受信する受信手順と、

初期値Z' =F(p, Y') を計算する初期値計算手順と、

次数r を取得する次数取得手順と、

当該初期値Z' にチェビシェフ写像T(r, ・) を繰り返し適用した所定の長さの擬似雑音系列

Z', T(r, Z'), T(r, T(r, Z')), T(r, T(r, T(r, Z'))), …

を出力する系列出力手順と、

を備えることを特徴とする出力方法。

【数９】

$$F(n, s(x)) = s(nx) \quad (n\text{は２以上の自然数})$$

【数１０】

$$T(n, \cos x) = \cos nx \quad (n\text{は２以上の自然数})$$

【請求項１１】前記次数取得手順にて取得する次数は、素数であることを特徴とする請求項１０記載の出力方法。

【請求項１２】あらかじめ設定した楕円関数s(・) と、実数X（ただし-1<;X<;1)と、［数１１］により定義される有理写像F(・, ・)と、［数１２］により定義されるチェビシェフ写像T(・, ・)とに基づいた擬似雑音系列の出力方法であって、自然数p を取得する自然数取得手順と、当該自然数p に基づいて値Y=F(p, X)を計算する送信値計算手順と、当該値Y を他の出力装置に送信する送信手順と、他の出力装置が送信した値Y' を受信する受信手順と、当該値Y' にまだ関数F(p, ・) を適用していない場合、値Y' ' =F(p, Y') を計算する第２の送信値計算手順と、当該値Y' ' を他の出力装置に送信する第２の送信手順と、当該値Y' に既に関数F(p, ・) を適用している場合、当該自然数q と当該値Y' に基いて初期値Z' =F(p, Y') を計算する初期値計算手順と、次数r を取得する次数取得手順と、当該初期値Z' にチェビシェフ写像T(r, ・) を繰り返し適用した所定の長さの擬似雑音系列Z', T(r, Z'), T(r, T(r, Z')), T(r, T(r, T(r, Z'))), …を出力する系列出力手順と、を備えることを特徴とする出力方法。

【数１１】

$$F(n, s(x)) = s(nx) \quad (n\text{は２以上の自然数})$$

【数１２】

$$T(n, \cos x) = \cos nx \quad (n\text{は２以上の自然数})$$

【請求項１３】前記次数取得手順にて取得する次数は、素数であることを特徴とする請求項１２記載の出力方法。

【請求項１４】あらかじめ設定した楕円関数s(・) と、実数X (ただし-1<;X<;1)と、［数１３］により定義される有理写像F(・,・)と、［数１４］により定義されるチェビシェフ写像T(・,・)とに基づいた擬似雑音系列を出力する処理を実現するプログラムを記録したコンピュータ読み取り可能な情報記録媒体であって、

自然数p を取得する自然数取得手順と、

値Y=F(p, X)を計算する送信値計算手順と、

当該値Y を第２の出力装置に送信する送信手順と、

前記第２の出力装置が送信した値Y' を受信する受信手順と、

初期値Z' =F(p, Y')を計算する初期値計算手順と、

次数r を取得する次数取得手順と、

当該初期値Z' にチェビシェフ写像T(r, ・) を繰り返し適用した所定の長さの擬似雑音系列

Z', T(r, Z'), T(r, T(r, Z')), T(r, T(r, T(r, Z'))), …

を出力する系列出力手順と、

を備える処理を実現するプログラムを記録することを特徴とする情報記録媒体。

【数１３】

$$F(n, s(x)) = s(nx) \quad (n\text{は２以上の自然数})$$

【数１４】

$$T(n, \cos x) = \cos nx \quad (n\text{は２以上の自然数})$$

【請求項１５】前記次数取得手順にて取得する次数は、素数であることを特徴とする請求項１４記載の情報記録媒体。

【請求項１６】あらかじめ設定した楕円関数s(・) と、実数X (ただし-1<;X<;1)と、［数１５］により定義される有理写像F(・,・)と、［数１６］により定義されるチェビシェフ写像T(・,・)とに基づいた擬似雑音系列を出力する処理を実現するプログラムを記録したコンピュータ読み取り可能な情報記録媒体であって、

自然数p を取得する自然数取得手順と、

当該自然数p に基づいて値Y=F(p, X)を計算する送信値計算手順と、

当該値Y を他の出力装置に送信する送信手順と、

他の出力装置が送信した値Y' を受信する受信手順と、

当該値Y' にまだ関数F(p, ・) を適用していない場合、値Y'' =F(p, Y') を計算する第２の送信値計算手順と、

当該値Y'' を他の出力装置に送信する第２の送信手順と、

当該値Y' に既に関数F(p, ・) を適用している場合、当該自然数ｑと当該値Y' に基いて初期値Z' =F(p, Y')を計算する初期値計算手順と、

次数r を取得する次数取得手順と、

当該初期値Z' にチェビシェフ写像T(r, ・) を繰り返し適用した所定の長さの擬似雑音系列

Z', T(r, Z'), T(r, T(r, Z')), T(r, T(r, T(r, Z'))), …

を出力する系列出力手順と、

を備える処理を実現するプログラムを記録したことを特徴とする情報記録媒体。

【数１５】

$$F(n, s(x)) = s(nx) \quad (n\text{は２以上の自然数})$$

【数１６】

$$T(n, \cos x) = \cos nx \quad (n\text{は２以上の自然数})$$

【請求項１７】前記次数取得手順にて取得する次数は、素数であることを特徴とする請求項１６記載の情報記録媒体。

【請求項１８】前記情報記録媒体は、コンパクトディスク、フロッピー（登録商標）ディスク、ハードディスク、光磁気ディスク、ディジタルビデオディスク、磁気テープ、または、半導体メモリであることを特徴とする請求項１４から１６記載の情報記録媒体。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、ＰＮ（Pseudorandom Noise；擬似雑音）系列を出力する出力システム、出力装置、出力方法、および、情報記録媒体に関する。特に、衛星通信、固定通信、携帯電話やＰＨＳ（Personal Handyphone System）などの陸上移動通信、ＧＰＳ（Global Positioning System）などの測距分野で用いるこ

とができるスペクトラム拡散通信のＣＤＭＡ（Code Division Multiple Access ：符号分割多元接続）方式の拡散符号として使用できるＰＮ系列を出力するのに好適な出力システム、出力装置、出力方法、および、情報記録媒体に関する。

【０００２】

【従来の技術】ＣＤＭＡ方式を用いるスペクトラム拡散通信などでは、ＰＮ系列を拡散符号として用いることにより、秘話性を高くし、帯域の利用効率をあげている。

【０００３】従来、ＰＮ系列としては、Ｍ系列、Ｇｏｌｄ符号、嵩符号などが利用されていた。これらの系列は、シフトレジスタやこれと排他的論理和回路を組み合わせることにより計算することができるが、２値系列を基本とするため、通信セキュリティを確保することが難しかった。

【０００４】一方で、スペクトラム拡散通信では、通信を行う端末の間で同期をとる必要があるが、通信セキュリティを高めることと同期を容易に行うこととは互いにトレードオフの関係にある。

【０００５】

【発明が解決しようとする課題】しかしながら、これら従来のＰＮ系列よりもさらに秘話性を高めることができるＰＮ系列を出力する手法が産業界から望まれている。特に、近年発展が目覚ましいカオス理論に基づいて、同定の難しいＰＮ系列を出力し、これをＣＤＭＡ方式の拡散符号として用いてスペクトラム拡散通信の秘話性を高める手法に対する要望は大きい。

【０００６】一方、カオス理論に基づいたＰＮ系列を単純に用いるのでは、通信の受信側で同期をとる際に、拡散符号をサーチすべき空間が莫大になるため、同期を容易に行う手法が望まれている。

【０００７】本発明は、以上のような問題を解決するためになされたもので、ＰＮ系列を出力する出力システム、出力装置、出力方法、および、情報記録媒体を提供することを目的とする。特に、スペクトラム拡散通信の拡散符号として使用できるＰＮ系列を出力するのに好適な出力システム、出力装置、出力方法、および、情報記録媒体を提供することを目的とする。

【０００８】

【課題を解決するための手段】以上の目的を達成するため、本発明の原理にしたがって、下記の発明を開示する。

【０００９】本発明のＰＮ系列の出力システムは、あらかじめ設定した楕円関数s(・) と、実数X（ただし-1<X<1)と、［数１７］により定義される有理写像F(・,・)と、［数１８］により定義されるチェビシェフ写像T(・,・)とに基づいた、自然数取得部と、送信値計算部と、送信部と、受信部と、次数取得部と、初期値計算部と、系列出力部とを備える第１および第２の出力装置を有するＰＮ系列の出力システムである。

【００１０】第１の出力装置の自然数取得部は、自然数 p を取得し、送信値計算部は、値Y=F(p, X)を計算し、送信部は、当該値Y を第２の出力装置に送信する。

【００１１】第２の出力装置の自然数取得部は、自然数 q を取得し、受信部は、第１の出力装置が送信した値Y を受信し、初期値計算部は、初期値Z=F(q, Y)を計算し、次数取得部は、次数s を取得し、系列出力部は、当該初期値Z にチェビシェフ写像T(s, ・) を繰り返し適用した所定の長さのＰＮ系列

Z, T(s, Z), T(s, T(s, Z)), T(s, T(s, T(s, Z))), …

を出力し、送信値計算部は、値Y'=F(q, X) を計算し、送信部は、当該値Y' を第１の出力装置に送信する。

【００１２】第１の出力装置の受信部は、第２の出力装置が送信した値Y' を受信し、初期値計算部は、初期値Z'=F(p, Y')を計算し、次数取得部は、次数r を取得し、系列出力部は、当該初期値Z' にチェビシェフ写像T(r, ・)を繰り返し適用した所定の長さのＰＮ系列

Z', T(r, Z'), T(r, T(r, Z')), T(r, T(r, T(r, Z'))), …

を出力するように構成する。

【００１３】

【数１７】

$$F(n, s(x)) = s(nx) \quad (n\text{は２以上の自然数})$$

【００１４】

【数１８】

$$T(n, \cos x) = \cos nx \quad (n\text{は２以上の自然数})$$

【００１５】また、本発明のＰＮ系列の出力システムでは、第１および第２の出力装置の次数取得部が取得する次数は、素数であるように構成することができる。

【００１６】本発明のＰＮ系列の出力装置は、あらかじめ設定した楕円関数s(・) と、実数X（ただし-1<X<1)と、［数１７］により定義される有理写像F(・,・)と、［数１８］により定義されるチェビシェフ写像T(・,・)とに基づいたＰＮ系列の出力装置である。

【００１７】この出力装置は、自然数p を取得する自然数取得部と、値Y=F(p, X)を計算する送信値計算部と、当該値Y を第２の出力装置に送信する送信部と、第２の出力装置が送信した値Y' を受信する受信部と、初期値Z'=F(p, Y')を計算する初期値計算部と、次数r を取得する次数取得部と、当該初期値Z' にチェビシェフ写像T(r, ・)を繰り返し適用した所定の長さのＰＮ系列

Z', T(r, Z'), T(r, T(r, Z')), T(r, T(r, T(r, Z'))), …

を出力する系列出力部と、を備えるように構成する。

【００１８】また、本発明の出力装置の次数取得部が取

得する次数は、素数であるように構成することができる。

【００１９】本発明のＰＮ系列の出力システムは、あらかじめ設定した楕円関数s(・) と、実数X (ただし-1<;X<;1)と、［数１７］により定義される有理写像F(・,・)と、［数１８］により定義されるチェビシェフ写像T(・,・)とに基づいた複数の出力装置を有するＰＮ系列の出力システムである。

【００２０】この出力システムが有する複数の出力装置のそれぞれは、自然数p を取得する自然数取得部と、値Y=F(p,X)を計算する送信値計算部と、当該値Y を他の出力装置に送信する送信部と、他の出力装置が送信した値Y'を受信する受信部と、当該値Y'にまだ関数F(p,・) を適用していない場合、値Y''=F(p,Y') を計算する第２の送信値計算部と、当該値Y'' を他の出力装置に送信する第２の送信部と、当該値Y'に既に関数F(p,・) を適用している場合、初期値Z'=F(p,Y')を計算する初期値計算部と、次数r を取得する次数取得部と、当該初期値Z'にチェビシェフ写像T(r,・) を繰り返し適用した所定の長さのＰＮ系列

Z', T(r,Z'), T(r,T(r,Z')), T(r,T(r,T(r,Z'))), …

を出力する系列出力部と、を備えるように構成する。

【００２１】また、本発明の出力システムでは、出力装置のそれぞれの自然数取得部が取得する次数は、素数であるように構成することができる。

【００２２】また、本発明の出力システムでは、出力装置は複数の群に分類され、同じ群に属する出力装置の自然数取得部が取得する次数は、同じ自然数であるように構成することができる。

【００２３】また、本発明の出力システムでは、出力装置は複数の群に分類され、同じ群に属する出力装置の送信値計算部に入力される実数は同じ実数であるように構成することができる。

【００２４】本発明のＰＮ系列の出力装置は、あらかじめ設定した楕円関数s(・) と、実数X (ただし-1<;X<;1)と、［数１７］により定義される有理写像F(・,・)と、［数１８］により定義されるチェビシェフ写像T(・,・)とに基づいたＰＮ系列の出力装置である。

【００２５】この出力装置は、自然数p を取得する自然数取得部と、当該自然数p に基づいて値Y=F(p,X)を計算する送信値計算部と、当該値Y を他の出力装置に送信する送信部と、他の出力装置が送信した値Y'を受信する受信部と、当該値Y'にまだ関数F(p,・) を適用していない場合、値Y''=F(p,Y') を計算する第２の送信値計算部と、当該値Y'' を他の出力装置に送信する第２の送信部と、当該値Y'に既に関数F(p,・) を適用している場合、当該自然数q と当該値Y'に基いて初期値Z'=F(p,Y')を計算する初期値計算部と、次数r を取得する次数取得部と、当該初期値Z'にチェビシェフ写像T(r,・) を繰り返し適用した所定の長さのＰＮ系列

Z', T(r,Z'), T(r,T(r,Z')), T(r,T(r,T(r,Z'))), …

を出力する系列出力部と、を備えるように構成する。

【００２６】また、本発明の出力装置の次数取得部が取得する次数は、素数であるように構成することができる。

【００２７】本発明のＰＮ系列の出力方法は、あらかじめ設定した楕円関数s(・) と、実数X (ただし-1<;X<;1)と、［数１７］により定義される有理写像F(・,・)と、［数１８］により定義されるチェビシェフ写像T(・,・)とに基づいたＰＮ系列の出力方法である。

【００２８】この出力方法は、自然数p を取得する自然数取得手順と、値Y=F(p,X)を計算する送信値計算手順と、当該値Y を第２の出力装置に送信する送信手順と、第２の出力装置が送信した値Y'を受信する受信手順と、初期値Z'=F(p,Y')を計算する初期値計算手順と、次数r を取得する次数取得手順と、当該初期値Z'にチェビシェフ写像T(r,・) を繰り返し適用した所定の長さのＰＮ系列

Z', T(r,Z'), T(r,T(r,Z')), T(r,T(r,T(r,Z'))), …

を出力する系列出力手順と、を備えるように構成する。

【００２９】また、本発明の出力方法の次数取得手順にて取得する次数は、素数であるように構成することができる。

【００３０】本発明のＰＮ系列の出力方法は、あらかじめ設定した楕円関数s(・) と、実数X (ただし-1<;X<;1)と、［数１７］により定義される有理写像F(・,・)と、［数１８］により定義されるチェビシェフ写像T(・,・)とに基づいたＰＮ系列の出力方法である。

【００３１】この出力方法は、自然数p を取得する自然数取得手順と、当該自然数p に基づいて値Y=F(p,X)を計算する送信値計算手順と、当該値Y を他の出力装置に送信する送信手順と、他の出力装置が送信した値Y'を受信する受信手順と、当該値Y'にまだ関数F(p,・) を適用していない場合、値Y''=F(p,Y') を計算する第２の送信値計算手順と、当該値Y'' を他の出力装置に送信する第２の送信手順と、当該値Y'に既に関数F(p,・) を適用している場合、当該自然数q と当該値Y'に基いて初期値Z'=F(p,Y')を計算する初期値計算手順と、次数r を取得する次数取得手順と、当該初期値Z'にチェビシェフ写像T(r,・) を繰り返し適用した所定の長さのＰＮ系列

Z', T(r,Z'), T(r,T(r,Z')), T(r,T(r,T(r,Z'))), …

を出力する系列出力手順と、を備えるように構成する。

【００３２】また、本発明の出力方法の次数取得手順にて取得する次数は、素数であるように構成することができる。

【００３３】本発明のＰＮ系列の出力システム、出力装置、出力方法を実現するプログラムをコンパクトディスク、フロッピーディスク、ハードディスク、光磁気ディスク、ディジタルビデオディスク、磁気テープ、半導体メモリなどの情報記録媒体に記録することができる。

【００３４】本発明の情報記録媒体に記録されたプログラムを、記憶装置、計算装置、出力装置などを備える汎用コンピュータや並列計算機などの情報処理装置で実行することにより、上記のＰＮ系列の出力システム、出力装置、出力方法を実現することができる。

【００３５】また、情報処理装置とは独立して、本発明のプログラムを記録した情報記録媒体を配布、販売することができる。

【００３６】

【発明の実施の形態】以下に本発明の一実施形態を説明する。なお、以下に説明する実施形態は説明のためのものであり、本願発明の範囲を制限するものではない。したがって、当業者であればこれらの各要素もしくは全要素をこれと均等なものに置換した実施形態を採用することが可能であるが、これらの実施形態も本願発明の範囲に含まれる。

【００３７】（第１の実施の形態）図１は、本発明のＰＮ系列の出力システムの構成を示す模式図（データフロー図）である。なお、図１は、上下方向の矢印の順に実行されるフローチャートとして見ることもできる。以下、図１を参照して説明する。

【００３８】出力システム１０１は、出力装置１１１と出力装置１６１とを有する。

【００３９】出力装置１１１は、自然数取得部１１２と、送信値計算部１１３と、送信部１１４と、受信部１１５と、初期値計算部１１６と、次数取得部１１７と、系列出力部１１８と、を備える。

【００４０】一方、出力装置１６１は、自然数取得部１６２と、送信値計算部１６３と、送信部１６４と、受信部１６５と、初期値計算部１６６と、次数取得部１６７と、系列出力部１６８と、を備える。

【００４１】出力装置１１１の自然数取得部１１２と、出力装置１６１の自然数取得部１６２と、は、それぞれ、ある程度大きな自然数p と自然数q とを取得する。これらの自然数は、秘密鍵として機能する。

【００４２】出力装置１１１と出力装置１６１との間では、あらかじめ設定された楕円関数s(・) と、所定の精度保証をした実数の公開鍵X (-1<;X<;1)とが共有されている。ここで、楕円関数s(・) と公開鍵X が傍受されても、後述するように通信セキュリティが下がることはない。

【００４３】出力装置１１１の送信値計算部１１３と、出力装置１６１の送信値計算部１６３と、は、それぞれ、自然数取得部１１２が取得した自然数p と自然数取得部１６２が取得した自然数q とから、それぞれ、値Y=F(p, X)と値Y'=F(q, X) とを計算する。

【００４４】ここで、写像F(・, ・)は楕円関数によって定義される有理写像であり、有理多項式によって直接表現することができる。すなわち、送信値計算部１１３と、送信値計算部１６３と、は、加減乗除を行う電子回路や、コンピュータのＣＰＵ（Central Processing Unit ；中央処理ユニット）とメモリなどとの結合により、容易に実現することができる。

【００４５】出力装置１１１の送信部１１４と、出力装置１６１の送信部１６４と、は、それぞれ、出力装置１６１の受信部１６５と、出力装置１１１の受信部１１５と、に、値Y と値Y' とを送信する。値Y と値Y' とが傍受されても、後述するように通信セキュリティが下がることはない。

【００４６】出力装置１１１の初期値計算部１１６と、出力装置１６１の初期値計算部１６６と、は、それぞれ、出力装置１１１の受信部１１５と、出力装置１６１の受信部１６５と、が受信した値Y' と、値Y と、に基づいて、初期値Z'=F(p, Y')と、初期値Z=F(q, Y)とを計算する。

【００４７】ここで、有理写像F(・, ・)は、楕円関数s(・) の加法定理により定義されているため、以下のような性質が成立する。

Z'=F(p, Y')=F(p, F(q, X))=F(q, F(p, X))=F(q, Y)=Z'

【００４８】このようにして、出力装置１１１と、出力装置１６１と、は、ＣＤＭＡ方式の拡散符号の初期値を共有することができる。

【００４９】出力装置１１１の次数取得部１１７と、出力装置１６１の次数取得部１６７と、は、それぞれ、次数r と、次数s と、を取得する。次数は、２以上の自然数であり、素数であることが望ましい。

【００５０】出力装置１１１の系列出力部１１８と、出力装置１６１の系列出力部１６８と、は、それぞれ、チェビシェフ写像T(r, ・) と、チェビシェフ写像T(s, ・) と、を値Z=Z' に繰り返し適用した以下の所定の長さのＰＮ系列

Z, T(r, Z), T(r, T(r, Z)), T(r, T(r, T(r, Z))), …

Z, T(s, Z), T(s, T(s, Z)), T(s, T(s, T(s, Z))), …

を出力する。このＰＮ系列は、漸化式による繰り返し計算で出力することが可能である。

【００５１】チェビシェフ写像の具体例を図２に示す。図２には、次数２から５のチェビシェフ写像T(2, ・) 、T(3, ・) 、T(4, ・) 、および、T(5, ・) がグラフ表示されている。チェビシェフ写像は、区間(-1, 1)を区間(-1, 1)に写像する有理写像であり、余弦関数の加法定理により定義することができるが、有理多項式で直接表現することもできる。［数１９］は次数２の、［数２０］は次数３の、チェビシェフ写像の多項式表現である。

【００５２】

【数１９】

$$T(2,y) = 2y^2 - 1$$

【００５３】

【数２０】

$$T(3,y) = 4y^3 - 3y$$

【００５４】したがって、系列出力部１１８と、系列出力部１６８と、は、加減乗除を行う電子回路や、コンピュータのＣＰＵとメモリなどとの結合により、容易に実現することができる。

【００５５】これらのＰＮ系列をＣＤＭＡ方式の拡散符号として用いた場合、相関関数がほぼ直交し、相関特性が、従来のＭ系列、Ｇｏｌｄ符号、嵩符号と比較して良好であることが、発明者らによって発見されている（K. Umeno and K. Kitayama, Electoronics Letters (1999) Vol. 35, pp.545-546 ； K. Umeno and K. Kitayama, to appear in Proc. 1999 IEEE Information Theory Workshop））。

【００５６】この後、出力装置１１１を備える通信装置（図示せず）と、出力装置１６１を備える通信装置（図示せず）と、は、それぞれ上記のＰＮ系列により、スペクトラム拡散を行って通信する。

【００５７】出力装置１１１を備える通信装置と、出力装置１６１を備える通信装置と、は、それぞれ、上記のＰＮ系列によりスペクトラム拡散された信号を受信することになる。この際にＣＤＭＡ方式の同期が必要になるが、上記のＰＮ系列は、チェビシェフ写像の次数が異なるだけなので、同期のサーチ空間を狭くすることができる。また、このチェビシェフ多項式によって生成された拡散符号の相関特性は、相関関数の意味で直交しているため、相関検波などを施すことにより容易に同期をとることができる。

【００５８】一方、楕円関数s(・)、公開鍵X、値Y、値Y'、のような情報を傍受されても、他者がＰＮ系列の初期値Z=Z'やＰＮ系列そのものを推測することは、楕円Diffe-Hellman 問題と同等の問題となる。この問題は、解くことがきわめて難しいことが知られている（N. コブリッツ, 櫻井幸一訳, 数論アルゴリズムと楕円暗号理論入門, シュプリンガー・フェアラーク東京, 1997）。

【００５９】これにより、カオスを用いた拡散符号により既存のＣＤＭＡ方式で用いられる拡散符号よりも通信セキュリティを高くする一方で、同期を容易にする、という２つの目的を達成することができる。

【００６０】ここで、公開鍵X として有理数を利用する場合、初期値も有理数となるため、出力装置１１１と出力装置１６１とが計算した初期値は厳密に一致（Z=Z'）する。一方、公開鍵X として浮動小数点数などを利用する場合には、十分高い精度を保っておけば、初期値を一致させることができる。この場合、公開鍵X から、共有される初期値Z=Z'までは、ディジタル情報として処理される。

【００６１】なお、本発明の出力装置１１１と、出力装置１６１と、は、いずれも、送受信を行う通信部（送信部１１４、受信部１１５、および、送信部１６４、受信部１６５）と、それ以外の処理を行う部分とに分けることができる。

【００６２】このうち、通信部以外の部分は、加減乗除などを行う電子回路により構成することが可能であり、一体化されたチップとして実装することができる。また、通信部以外の部分は、ＣＰＵやメモリを有するコンピュータにより実装することもできる。これらは当業者であれば公知の技術により容易に実装することができ、これらの実施形態は本発明の範囲に含まれる。

【００６３】（第２の実施の形態）第１の実施形態は、１対１のＣＤＭＡ方式のスペクトラム拡散通信において利用できる拡散符号をカオスにより出力するものであったが、本実施形態は、複数のユーザ、特に、３人以上のユーザが相互に通信を行うような場合に適用することができる。

【００６４】図３は、本実施形態の出力システムで使用される出力装置の概要を示す模式図（データフロー図）である。なお、図３は、上下方向の矢印の順に実行されるフローチャートとして見ることもできる。

【００６５】本実施形態の出力装置３１１は、自然数取得部３１２と、送信値計算部３１３と、送信部３１４と、受信部３１５と、初期値計算部３１６と、次数取得部３１７と、系列出力部３１８と、第２の送信値計算部３２０と、第２の送信部３２１と、を備える。

【００６６】出力装置３１１の自然数取得部３１２は、ある程度大きな自然数p を取得する。この自然数は、秘密鍵として機能する。

【００６７】システム内で相互に通信する出力装置３１１の間では、あらかじめ設定された楕円関数s(・)と、所定の精度保証をした実数の公開鍵X (-1<;X<;1)とが共有されている。

【００６８】出力装置３１１の送信値計算部３１３は、自然数取得部３１２が取得した自然数p から値Y=F(p, X)を計算する。

【００６９】出力装置３１１の送信部３１４は、他の出力装置３１１の受信部３１５に、値Y を送信する。

【００７０】出力装置３１１の受信部３１５が、他の出力装置３１１から送信された値Y'を受信した場合、当該値Y'に、自身もすでに写像F(p, ・)を適用しており他の出力装置３１１もそれぞれの写像を適用しているか否かを判別する。

【００７１】まだ適用していない場合、第２の送信値計算部３２０は、値Y''=F(p, Y')を計算し、第２の送信部３２１は、当該値Y''を他の出力装置３１１に送信する。なお、第２の送信部３２１と送信部３１４とは、同じハードウェアを共通に利用して実現することができる。

【００７２】既に適用している場合、出力装置３１１の初期値計算部３１６は、初期値Z'=F(p, Y')を計算する。

【００７３】なお、この判別は、写像を適用した出力装置を識別する情報をY やY'' と合わせて相互に通信し、この情報を吟味することにより行うことができる。

【００７４】また、この判別は、たとえばユーザの数がK (K≧3)人である場合、図４に示すように、カウンタ３１９を設けて行うことができる。図４では、図３と共通の要素には同じ符号を付し、また、相違がない部分については図示を省略している。カウンタ３１９は、最初に０にクリアされ、他の出力装置３１１から送信された値を受信部３１５が受信するたびに１ずつインクリメントされる。

【００７５】カウンタ３１９で計数される値をK'と表すと、K'<K-2の場合、他の出力装置３１１のうち、まだ写像を適用していないものがあることになる。この場合は、Y'は他の出力装置３１１の送信部３１４によって送信されたことを起源とし、自身の送信部３１４から送信されたものではないため、第２の送信値計算部３２０により、自身の写像F(p, ・) を適用する。

【００７６】K'=K-2の場合、自身もすでに写像を適用しており、他の出力装置３１１もそれぞれの写像を適用していることになる。この場合は、カウンタ３１９の値を０にクリアして、初期値計算部３１６により初期値を計算させる。

【００７７】ここで、有理写像F(・, ・)は、ある特定の楕円関数s(・) の加法定理により定義されているため、すべての出力装置３１１の第２の送信値計算部３２０による写像が適用されていれば、すべての出力装置で初期値Z'は同じ値となる。

【００７８】これは、たとえば３者通信の場合、３つの出力装置３１１の自然数取得部がそれぞれp, q, t を取得したとすると、以下の性質が成立するからである。

F(p, F(q, F(t, X)))=F(p, F(t, F(q, X)))=F(q, F(p, F(t, X)))=F(q, F(t, F(p, X)))=F(t, F(p, F(q, X)))=F(t, F(q, F(p, X)))

これは、４者以上の通信の場合も同様である。

【００７９】このようにして、相互に通信する複数の出力装置３１１は、ＣＤＭＡ方式の拡散符号の初期値を共有することができる。この初期値（秘密鍵）共有の処理は、アナログ値をとる無線だけに限らず、光ファイバーなどを使うディジタル通信など、いずれの通信手段にも適用することができる。

【００８０】出力装置３１１の次数取得部３１７は、次数r を取得する。次数は、２以上の自然数であり、素数であることが望ましい。

【００８１】出力装置３１１の系列出力部３１８は、チェビシェフ写像T(r, ・) を値Z'に繰り返し適用した以下の所定の長さのＰＮ系列

Z', T(r, Z'), T(r, T(r, Z')), T(r, T(r, T(r, Z'))), …

を出力する。このＰＮ系列は、漸化式による繰り返し計算で出力することが可能である。

【００８２】この後、出力装置３１１を備える通信装置（図示せず）は、上記のＰＮ系列により、スペクトラム拡散を行って通信する。

【００８３】本実施形態においても、高い通信セキュリティを確保しつつ、同期が容易にできるという性質が得られるのは、第１の実施形態と同様である。

【００８４】（第３の実施形態）本実施形態は、第２の実施形態と同様に、多くのユーザの間でのＣＤＭＡ方式のスペクトラム拡散通信を実現する場合の実施形態であるが、ユーザが複数の群（グループ）に分類できるときに、このグループ内で前述した初期値（秘密鍵）共有の処理を行い、同じグループ以外のユーザとは干渉しないような拡散符号を構成できるものである。

【００８５】たとえば、グループの数が３つの場合、互いに異なる３種類の公開鍵をもとにして、それぞれが互いに異なる初期値（秘密鍵）をグループ内で共有する。各グループに属するユーザの出力装置３１１では、それぞれ異なる自然数を系列出力部３１８の計算の次数として用いる。グループの数が増減した場合も同様である。

【００８６】チェビシェフ写像では、初期値が異なる素数を採用した場合、出力されるＰＮ系列は、そのチェビシェフ写像の次数を問わず相関関数の意味で常に直交する。このため、互いのグループがこのＰＮ系列をＣＤＭＡ方式の拡散符号として使用しても、異なるグループの拡散符号が偶然に一致することはありえない。

【００８７】このため、グループ内では互いに通信を行うことができ、自身が属するグループ以外とは高い秘話性を持ち、同期をとることが難しいという特徴を持つ拡散符号を出力することができる。

【００８８】

【発明の効果】以上説明したように、本発明によれば、ＰＮ系列を出力する出力システム、出力装置、出力方法、および、情報記録媒体を提供することができる。特に、スペクトラム拡散通信のＣＤＭＡ方式の拡散符号として使用できるＰＮ系列を出力するのに好適な出力システム、出力装置、出力方法、および、情報記録媒体を提供することができる。

【図面の簡単な説明】

【図１】本発明のＰＮ系列の出力システムの第１の実施の形態の構成を示す模式図である。

【図２】チェビシェフ写像の様子を示すグラフである。

【図３】本発明のＰＮ系列の出力システムの第２の実施の形態の構成を示す模式図である。

【図４】本発明のＰＮ系列の出力システムの第２の実施の形態のカウンタなどの構成を示す模式図である。

【符号の説明】

１０１　出力システム

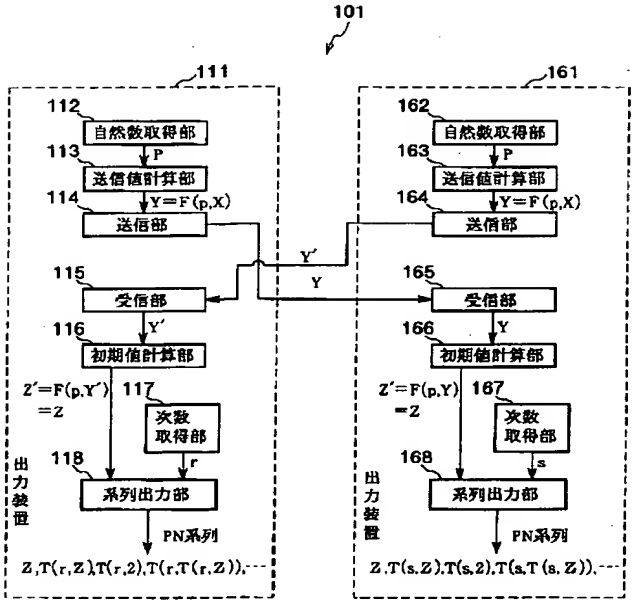
１１１　第１の出力装置

１１２　自然数取得部

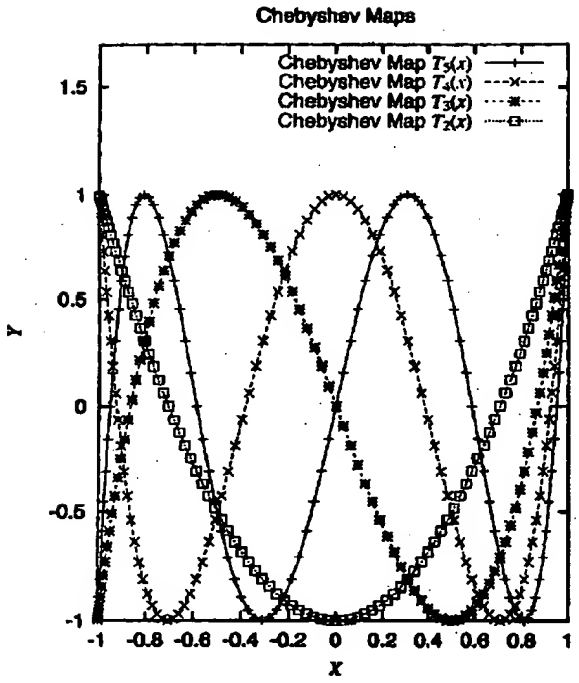
１１３　送信値計算部

１１４　送信部
１１５　受信部
１１６　初期値計算部
１１７　次数取得部
１１８　系列出力部
１６１　第２の出力装置
１６２　自然数取得部
１６３　送信値計算部
１６４　送信部
１６５　受信部
１６６　初期値計算部
１６７　次数取得部
１６８　系列出力部
３１１　出力装置
３１２　自然数取得部
３１３　送信値計算部
３１４　送信部
３１５　受信部
３１６　初期値計算部
３１７　次数取得部
３１８　系列出力部
３１９　カウンタ
３２０　第２の送信値計算部
３２１　第２の送信部

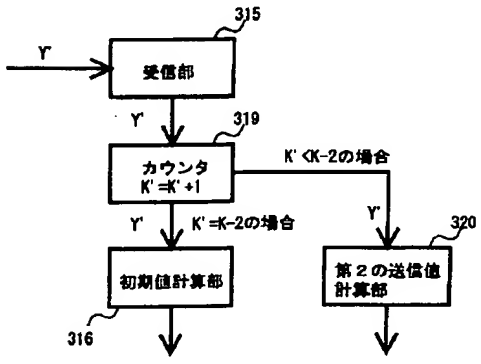
【図１】



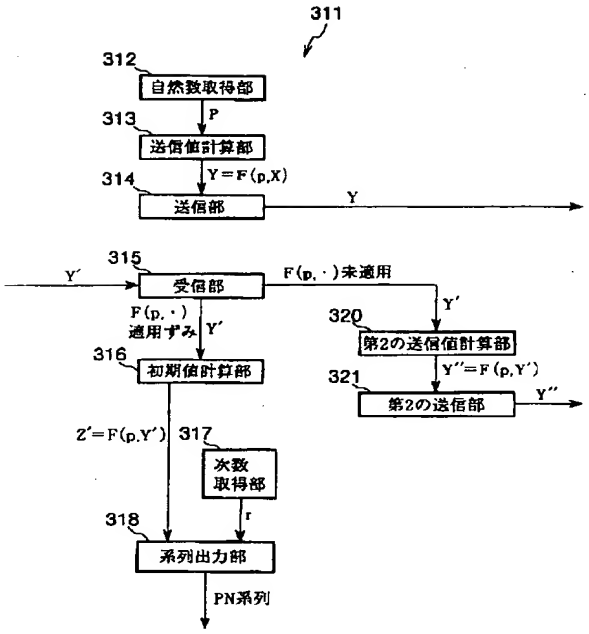
【図２】



【図４】



【図３】


311
312
自然数取得部
P
313
送信値計算部
Y＝F(p,X)
314
送信部
Y
Y′
315
受信部
F(p,・)未適用
Y′
F(p,・)
適用ずみ
Y′
320
第2の送信値計算部
Y″＝F(p,Y′)
321
第2の送信部
Y″
316
初期値計算部
Z′＝F(p,Y′)
317
次数
取得部
r
318
系列出力部
PN系列